EVALUATION REPORT

~~OFFICIAL USE ONLY~~

Information System Security
Evaluation of the Technical Training
Center – Chattanooga, TN

OIG-09-A-11 July 22, 2009

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

OFFICE OF THE
INSPECTOR GENERAL

July 22, 2009

MEMORANDUM TO: R. William Borchardt
Executive Director for Operations

FROM: Stephen D. Dingbaum /**RA**/
Assistant Inspector General for Audits

SUBJECT: INFORMATION SYSTEM SECURITY EVALUATION OF THE TECHNICAL TRAINING CENTER – CHATTANOOGA, TN (OIG-09-A-11)

Attached is the Office of the Inspector General's (OIG) report titled, *Information System Security Evaluation of the Technical Training Center – Chattanooga, TN*. The report presents the results of the subject evaluation.

Please provide information on actions taken or planned on each of the recommendations within 30 days of the date of this memorandum. Actions taken or planned are subject to OIG follow up as stated in Management Directive 6.1.

We appreciate the cooperation extended to us by members of your staff during the evaluation. If you have any questions or comments about our report, please contact me at 415-5915 or Beth Serepca, Team Leader, Security and Information Management Audit Team, at 415-5911.

Attachment: As stated

Electronic Distribution

Edward M. Hackett, Executive Director, Advisory Committee on Reactor Safeguards
E. Roy Hawkens, Chief Administrative Judge, Atomic Safety and Licensing Board Panel
Stephen G. Burns, General Counsel
Brooke D. Poole, Jr., Director, Office of Commission Appellate Adjudication
Jim E. Dyer, Chief Financial Officer
Margaret M. Doane, Director, Office of International Programs
Rebecca L. Schmidt, Director, Office of Congressional Affairs
Eliot B. Brenner, Director, Office of Public Affairs
Annette Vietti-Cook, Secretary of the Commission
R. William Borchardt, Executive Director for Operations
Bruce S. Mallett, Deputy Executive Director for Reactor and Preparedness Programs, OEDO
Martin J. Virgilio, Deputy Executive Director for Materials, Waste, Research, State, Tribal, and Compliance Programs, OEDO
Darren B. Ash, Deputy Executive Director for Corporate Management and Chief Information Officer, OEDO
Vonna L. Ordaz, Assistant for Operations, OEDO
Kathryn O. Greene, Director, Office of Administration
Cynthia A. Carpenter, Director, Office of Enforcement
Charles L. Miller, Director, Office of Federal and State Materials and Environmental Management Programs
Guy P. Caputo, Director, Office of Investigations
Thomas M. Boyce, Director, Office of Information Services
James F. McDermott, Director, Office of Human Resources
Michael R. Johnson, Director, Office of New Reactors
Michael F. Weber, Director, Office of Nuclear Material Safety and Safeguards
Eric J. Leeds, Director, Office of Nuclear Reactor Regulation
Brian W. Sheron, Director, Office of Nuclear Regulatory Research
Corenthis B. Kelley, Director, Office of Small Business and Civil Rights
Roy P. Zimmerman, Director, Office of Nuclear Security and Incident Response
Samuel J. Collins, Regional Administrator, Region I
Luis A. Reyes, Regional Administrator, Region II
Mark A. Satorius, Region III
Elmo E. Collins, Jr., Regional Administrator, Region IV

Office of the Inspector General
Information System Security Evaluation of the Technical Training Center – Chattanooga, TN

Contract Number: GS-00F-0001N
Delivery Order Number: 20291

July 21, 2009

[Page intentionally left blank]

EXECUTIVE SUMMARY

BACKGROUND

The Nuclear Regulatory Commission's (NRC) Technical Training Center (TTC) was established in Chattanooga in 1980 as part of an expanded program of training based primarily on lessons learned from the Three Mile Island incident. Chattanooga was originally selected as the site for enhanced inspector training because of the need to make greater use in the agency's technical training programs of reactor simulators owned by the Tennessee Valley Authority. Since 1980, the NRC has purchased its own simulators and currently has four operating at the Chattanooga site.

On December 17, 2002, the President signed the E-Government Act of 2002, which included the Federal Information Security Management Act (FISMA) of 2002. FISMA outlines the information security management requirements for agencies, which include an annual independent evaluation of an agency's information security program[1] and practices to determine their effectiveness. This evaluation must include testing the effectiveness of information security policies, procedures, and practices for a representative subset of the agency's information systems. FISMA also requires assessment of compliance with FISMA requirements and related information security policies, procedures, standards, and guidelines. FISMA requires the annual evaluation to be performed by the agency's Inspector General or by an independent external auditor.

The NRC Office of the Inspector General (OIG) requested that the four NRC regional offices and the TTC be included in the independent evaluation of the agency's implementation of FISMA for fiscal year 2009. Information security policies, procedures, and practices at the regional offices and the TTC were last assessed in 2003 and 2006. This report describes evaluation findings for the TTC.

PURPOSE

The objectives of the information system security evaluation of the TTC were to:

- Evaluate the adequacy of NRC's information security program and practices for NRC automated information systems as implemented at the TTC.
- Evaluate the effectiveness of agency information security control techniques as implemented at the TTC.
- Evaluate corrective actions planned and taken as a result of previous OIG evaluations.

[1] For the purposes of FISMA, the agency uses the term "information system security program."

RESULTS IN BRIEF

The TTC has made improvements in its implementation of NRC's information system security program and practices for NRC automated information systems since the previous evaluations in 2003 and 2006. All corrective actions from the previous evaluations have been implemented. However, the information system security practices are not always consistent with the NRC's automated information systems security program as defined in Management Directive (MD) and Handbook 12.5, *NRC Automated Information Systems Security Program*, other NRC policies, FISMA, and National Institute of Standards and Technology (NIST) guidance. While many of the TTC's automated and manual security controls are generally effective, some security controls need improvement.

Physical and Environmental Security Controls

Overall, the TTC is implementing the physical and environmental security controls described in MD and Handbook 12.1, *NRC Facility Security Program*; MD and Handbook 12.5; and NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*. The TTC has implemented a number of safeguards to restrict access to the facility, including visitor access controls and new physical access control systems. Fire suppression and detection systems are adequate and meet NRC requirements. Environmental controls are sufficient to protect information technology (IT) equipment from potential hazards. Short-term uninterruptible power supplies provide sufficient power to facilitate an orderly shutdown of IT equipment in the event of a primary power source loss.

However, the TTC is not reviewing physical access logs or monitoring real-time physical intrusion alarms and surveillance equipment as required by MD and Handbook 12.5 and NIST SP 800-53. The agency provided TTC staff insufficient training and documentation on the new physical access controls systems installed at the TTC due to delays in completing the installation of the badge access system at the TTC. As a result, the TTC may be unable to detect, respond to, or investigate potential unauthorized access to its facility.

Continuity of Operations and Emergency Planning

The majority of the TTC's procedures for maintaining continuity of operations and for emergency planning are consistent with the requirements in MD and Handbook 12.1, MD and Handbook 12.5, and NIST SP 800-53. The TTC has documented backup procedures and developed contingency plans for local area network equipment as well as IT equipment supporting the simulators and the TTC's automated information systems. The TTC has developed a site-specific Occupant Emergency Plan as well as a physical security plan for the protection of safeguards information.

However, the evaluation team identified issues with the TTC backup procedures for the Windows and Novell infrastructure servers and the new badge access system.

Specifically, some information system backup information is not stored offsite, and there are no documented backup procedures for the badge access system. As a result, the TTC may not have reliable information system backup information on hand if there is a need for system or file recovery.

Configuration Management

In order to evaluate the TTC's compliance with the agency's configuration management requirements, the evaluation team asked TTC staff questions about the implementation of the agency's new laptop security policy. The evaluation team also conducted a network vulnerability assessment scan. As the TTC is just beginning to implement the requirements outlined in the new laptop security policy, the evaluation team was unable to form an opinion on its progress. However, the network vulnerability assessment scan identified deviations from the agency's configuration requirements.

FISMA and NIST SP 800-53 require agencies to develop policies and procedures that ensure compliance with minimally acceptable system configuration requirements as determined by the agency. The NRC's minimally acceptable system configuration requirements are based on various industry standards. However, a network vulnerability assessment scan identified several vulnerabilities that indicate some TTC systems are not configured in accordance with the agency's established configuration requirements.

RECOMMENDATIONS

This report makes recommendations to the Executive Director for Operations to improve NRC's information system security program and implementation of FISMA at the TTC. A consolidated list of recommendations appears on page 13 of this report.

[Page intentionally left blank]

ABBREVIATIONS AND ACRONYMS

Carson Associates	Richard S. Carson and Associates, Inc.
DFS	Division of Facilities and Security
DISA	Defense Information Systems Agency
FISMA	Federal Information Security Management Act
FY	Fiscal Year
HSPD-12	Homeland Security Presidential Directive-12
IT	Information Technology
LAN	Local Area Network
MD	Management Directive
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
OIG	Office of the Inspector General
SP	Special Publication
SSL	Secure Socket Layer
TLS	Transport Layer Security
TTC	Technical Training Center

[Page intentionally left blank]

TABLE OF CONTENTS

[Page intentionally left blank]

1 Background

The Nuclear Regulatory Commission's (NRC) Technical Training Center (TTC) was established in Chattanooga in 1980 as part of an expanded program of training based primarily on lessons learned from the Three Mile Island incident. Chattanooga was originally selected as the site for enhanced inspector training because of the need to make greater use in the agency's technical training programs of reactor simulators owned by the Tennessee Valley Authority. Since 1980, the NRC has purchased its own simulators and currently has four operating at the Chattanooga site.

The TTC provides training to meet staff needs in the curriculum areas of reactor technology, probabilistic risk assessment, engineering support, radiation protection, fuel cycle, security and safeguards, and regulatory skills. A spectrum of classroom and simulator courses is provided to meet the cumulative regulatory and technical training needs of the NRC headquarters and regional staff. The TTC is a part of the Office of Human Resources and operates under the direction of the Associate Director for Training and Development.

On December 17, 2002, the President signed the E-Government Act of 2002, which included the Federal Information Security Management Act (FISMA) of 2002.[2] FISMA outlines the information security management requirements for agencies, which include an annual independent evaluation of an agency's information security program and practices to determine their effectiveness. This evaluation must include testing the effectiveness of information security policies, procedures, and practices for a representative subset of the agency's information systems. FISMA requires the annual evaluation to be performed by the agency's Inspector General or by an independent external auditor.

The NRC Office of the Inspector General (OIG) requested that the four NRC regional offices and the TTC be included in the independent evaluation of the agency's implementation of FISMA for fiscal year (FY) 2009. Information security policies, procedures, and practices at the regional offices and the TTC were last assessed in 2003 and 2006. Richard S. Carson and Associates, Inc. (Carson Associates), performed the independent evaluation of NRC's implementation of FISMA for FY 2009 and performed the information system security evaluation of the TTC, and this report describes the results of that effort.

The information system security evaluation focused on the following elements of the agency's information security program and practices:

- Security policies and procedures.
- Automated information systems inventory.
- Physical and environmental security controls.
- Continuity of operations and emergency planning.

[2] The Federal Information Security Management Act of 2002 was enacted on December 17, 2002, as part of the E-Government Act of 2002 (Public Law 107-347) and replaces the Government Information Security Reform Act, which expired in November 2002.

- Configuration management.
- Local area network (LAN) administration.

2 Purpose

The objectives of the information system security evaluation of the TTC were to:

- Evaluate the adequacy of NRC's information security program and practices for NRC automated information systems as implemented at the TTC.
- Evaluate the effectiveness of agency information security control techniques as implemented at the TTC.
- Evaluate corrective actions planned and taken as a result of previous OIG evaluations.

The appendix contains a description of the evaluation scope and methodology.

3 Findings

The TTC has made improvements in its implementation of NRC's information system security program and practices for NRC automated information systems since the previous evaluations in 2003 and 2006. All corrective actions from the previous evaluations have been implemented. However, the information system security program and practices are not always consistent with the NRC's automated information systems security program as defined in Management Directive (MD) and Handbook 12.5, *NRC Automated Information Systems Security Program*, other NRC policies, FISMA, and National Institute of Standards and Technology (NIST) guidance. While many of the TTC's automated and manual security controls are generally effective, some security controls need improvement. Specifics on these matters are described in the following sections.

3.1 Physical and Environmental Security Controls

Overall, the TTC is implementing the physical and environmental security controls described in MD and Handbook 12.1, *NRC Facility Security Program*; MD and Handbook 12.5; and NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*. The TTC has implemented a number of safeguards to restrict access to the facility, including visitor access controls and new physical access control systems. Fire suppression and detection systems are adequate and meet NRC requirements. Environmental controls are sufficient to protect information technology (IT) equipment from potential hazards. Short-term uninterruptible power supplies provide sufficient power to facilitate an orderly shutdown of IT equipment in the event of a primary power source loss. However, the evaluation team identified issues with the installation of the new physical access control systems.

Access Logs Are Not Reviewed and Intrusion Alarms and Surveillance Equipment Are Not Monitored

The TTC is not reviewing physical access logs or monitoring real-time physical intrusion alarms and surveillance equipment as required by MD and Handbook 12.5 and NIST SP 800-53. The agency provided TTC staff insufficient training and documentation on the new physical access controls systems installed at the TTC due to delays in completing the installation of the badge access system at the TTC. As a result, the TTC may be unable to detect, respond to, or investigate potential unauthorized access to its facility.

3.1.1 Physical Access Control Systems

President George W. Bush issued Homeland Security Presidential Directive-12 (HSPD-12) on August 27, 2004, to address wide variations in the quality and security of forms of identification used to gain access to Federal facilities. This directive ordered the establishment of a mandatory governmentwide standard for secure and reliable forms of identification to be issued by the Government to its contractors and employees. One of HSPD-12's goals is that these identification badges be used for physical access to all Government facilities. Part of the agency's HSPD-12 solution is to replace the existing badge access systems at all NRC locations.

The TTC was the first location to receive the new badge access system, primarily because its existing system was no longer functioning. The installation began in October 2008, with a break in November, and was completed in December 2008. In addition to the badge access system, the agency installed an intrusion detection system, a closed-circuit surveillance system, and an intercom with an integrated video system.

However, the agency was not fully prepared for installing the new badge access system at the TTC. The TTC's badge access system server was not ready; subsequently, the agency temporarily installed the "global" badge access system server at the TTC. This global server is the server that will eventually serve as the primary badge access server for all of NRC. The Division of Facilities and Security (DFS), within the Office of Administration, had planned to return to the TTC in January 2009 to swap the global sever with TTC's server. However, DFS has been waiting since October 2008 for the TTC's server to be "hardened"[3] by the Office of Information Services.

3.1.2 Physical Access Requirements

MD and Handbook 12.5 detail the physical access controls required to protect the NRC buildings, facilities, and related supporting infrastructures that are housing essential IT resources, such as data centers, server rooms, the rooms that contain telecommunications equipment, wiring closets, and other IT equipment rooms. Specifically, MD and Handbook 12.5 Appendix A, "NRC Systems Development and Maintenance Security Controls," provide guidance for

[3] Hardening refers to the process of establishing minimally acceptable system configuration requirements for a server, then configuring the server in accordance with those requirements. The agency has established hardening specifications for the various devices, operating systems, and applications in use at the agency. These hardening standards can be found on the agency's internal Web site at http://www.internal.nrc.gov/CSO/standards.html.

reviewing physical access logs and monitoring real-time physical intrusion alarms and surveillance equipment.

MD and Handbook 12.5 Appendix A states that if a badge access system is used to control access, the system shall record all entries to the room and shall be capable of producing printed audit trails. Furthermore, the audit trails shall be maintained in either electronic or printed form for at least 2 months. NIST SP 800-53 requires organizations to (i) monitor physical access to information systems to detect and respond to physical security incidents and (ii) review physical access logs periodically and investigate apparent security violations or suspicious physical access activities.

MD and Handbook 12.5 Appendix A states that if an intrusion detection system is installed, the system shall detect unauthorized entry attempts, as well as motion or sound within the room. The intrusion detection system shall be programmed to activate an alarm at a security monitoring center that is staffed 24 hours a day. NIST SP 800-53 requires organizations to monitor real-time physical intrusion alarms and surveillance equipment.

3.1.3 Agency Has Not Met Requirements

The TTC is not reviewing physical access logs as required by MD and Handbook 12.5 and NIST SP 800-53 because the agency provided only brief training to TTC staff on monitoring activities on the TTC's new badge access system and did not provide any documentation. The TTC has tried to follow the written procedures TTC staff developed based on notes taken during the brief training provided during the installation, but staff have not been able to locate any access records or logs.

The TTC is not monitoring real-time physical intrusion alarms and surveillance equipment as required by MD and Handbook 12.5 and NIST SP 800-53. The agency provided no training on reviewing the video recordings captured by the closed-circuit surveillance system, and the intrusion detection system has not been activated and does not alarm at a security monitoring center that is staffed 24 hours a day.

3.1.4 Insufficient Training and Documentation

During the installation of the physical access control systems, the vendor performing the installation provided limited training to the TTC staff member responsible for administering these systems. The training was informal and was provided while the vendor was installing and configuring the systems. The training focused primarily on the badge access system and the process for adding employees and badges, assigning badges to employees, setting up access rights (via groups), and setting up access to the badge readers. The training only briefly covered monitoring badge access system activities and alarms. The training did not include procedures for performing system backups of the badge access system database.

The agency provided very minimal training to TTC staff on the other physical access control systems recently installed at the TTC. For example, the agency provided little training on the closed-circuit surveillance system and the intercom with an integrated video system. The only

procedure that was specifically discussed was resetting the closed-circuit surveillance system camera output display after a power loss. The agency provided no training on when and how to review the video recordings captured by the closed-circuit surveillance system.

The agency also provided no training on the intrusion detection system. The agency has stated that the intrusion detection system will not be activated until the installation of the complete suite of physical access control systems has been completed. Once the installation is completed, the agency will coordinate with the Federal Protective Service to monitor the alarms and the system will be activated.

In addition to insufficient training, the agency did not provide sufficient documentation for the new physical access control systems. In fact, the agency has not provided any written instructions for using any of the new physical access control systems. The TTC developed its own written procedures based on notes taken during the brief training provided during the installation. TTC staff also stated that they were not provided any manuals on the new hardware and software. Some relevant manuals were found in the trash left behind by the vendor who performed the installation.

3.1.5 Delay in Completing Installation

The insufficient training and documentation are a direct result of the delay in completing the installation of the badge access system at the TTC. The plan was to provide detailed follow up training and written instructions in January 2009 when the agency returned to the TTC to swap the global sever with TTC's server. However, due to the delay in the hardening of the TTC's badge access system server, DFS has yet to return to the TTC and has not provided a timeframe as to when the TTC's server will be ready for installation.

3.1.6 Unauthorized Access May Go Undetected

As a result of the delay in completing the installation of the TTC's badge access system and the insufficient training and documentation, unauthorized access to locations housing essential IT resources may go undetected. The TTC may be unable to detect, respond to, or investigate potential unauthorized access to its facility. As the TTC has not been given a timeframe as to when its server will be ready for installation, DFS should provide additional training and documentation on the new physical access control systems immediately.

A roving security patrol for the Osborne Office Center complex where the TTC is located is on duty during non-work hours. While the agency waits to coordinate with the Federal Protective Service to monitor alarms from the intrusion detection system, the agency should activate the system so that it sounds a local audible alarm that could be responded to by the roving security patrol during non-work hours.

RECOMMENDATIONS

The Office of the Inspector General recommends that the Executive Director for Operations:

1. Provide comprehensive training on the TTC's new physical access control systems as soon as possible. The agency should not wait until DFS returns to install the TTC's badge access system server.
2. Provide comprehensive documentation on the TTC's new physical access control systems as soon as possible. The agency should not wait until DFS returns to install the TTC's badge access system server.
3. Complete the hardening of the TTC's badge access system server and install it at the TTC.
4. Activate the TTC's intrusion detection system to sound a local audible alarm until the agency can coordinate with the Federal Protective Service to monitor the alarms.

3.2 Continuity of Operations and Emergency Planning

The majority of the TTC's procedures for maintaining continuity of operations and for emergency planning are consistent with the requirements in MD and Handbook 12.1, MD and handbook 12.5, and NIST SP 800-53. The TTC has documented backup procedures and developed contingency plans for LAN equipment as well as IT equipment supporting the simulators and the TTC's automated information systems. The TTC has developed a site-specific Occupant Emergency Plan as well as a physical security plan for the protection of safeguards information. However, the evaluation team identified issues with the TTC backup procedures for the Windows and Novell infrastructure servers and the new badge access system.

Backup Procedures Are Not Complete

MD and Handbook 12.5 Appendix A, "NRC Systems Development and Maintenance Security Controls," and NIST SP 800-53 detail requirements for backups of automated information systems. However, the agency has not met all the requirements. Specifically, some information system backup information is not stored offsite, and there are no documented backup procedures for the badge access system. As a result, the TTC may not have reliable information system backup information on hand if there is a need for system or file recovery.

3.2.1 Backup Requirements

MD and Handbook 12.5 Appendix A, "NRC Systems Development and Maintenance Security Controls," details requirements for backups of automated information systems, and states that these procedures should be implemented when backing up media to ensure that reliable backups are on hand if there is a need for system or file recovery. These procedures include, but are not limited to:

- Backup schedule – outlines the type of backup, the interval for each backup, the storage location, and the number of copies of each backup.

- Full backups – performed at least weekly.
- Incremental (differential) backups – performed nightly.
- Location of backups – at least two full backups maintained. One should remain onsite and a second copy should be removed to an offsite storage facility immediately after its creation.
- Backup media – use high-quality media to ensure good quality backups are available for recovery should the need arise.
- Storage of backups – store both onsite and offsite backups in a location, cabinet, or safe that is waterproof and fireproof for at least 14 days or as recommended by the agency.
- Testing of storage – backups are periodically tested to ensure they can be used effectively to restore sensitive information.

NIST SP 800-53 requires organizations to identify an alternate storage site for the storage of information system backup information, and requires the alternate storage site to be geographically separated from the primary storage site so as not to be susceptible to the same hazards.

3.2.2 Agency Has Not Met Requirements

The TTC has developed a contingency plan and backup procedures for the Windows and Novell infrastructure servers. Full backups of the infrastructure servers are conducted every Friday, and a specialized backup procedure is in place to backup users' electronic mailboxes. Data from these processes are written to a tape library. In addition, the TTC performs a redundant backup of its Novell infrastructure servers. Data from this backup process is written to removable, encrypted hard drives. Every Thursday, one of the encrypted hard drives containing the redundant Novell backup data is sent offsite. However, tapes from the tape library are never sent offsite.

The agency has not provided the TTC with any documented backup procedures for the new badge access system. The vendor performed a backup during a recent visit to repair a faulty badge reader; however, additional backups have not been performed since that time. The lack of documented backup procedures for the badge access system is a direct result of the delay in completing the installation of the badge access system at the TTC.

3.2.3 Potential Risk of Data Loss

Should there be an event (e.g., a fire) that causes significant damage to the main TTC computer room, the onsite backup tapes could be damaged or destroyed. The majority of the Windows infrastructure servers could be restored without backups. The Novell servers could be restored from the offsite backup data stored on the removable hard drives. However, the contents of the TTC users' electronic mailboxes would be lost.

As backup procedures for the badge access system server are not documented at all, backups are performed only on an ad hoc basis. Backups of the badge access system need to be performed regularly to meet agency and NIST requirements and preserve data in the event of a system

failure. Should there be an event that causes damage to the badge access system server (e.g., a fire, damaged hard drive), the TTC would have to re-enter all the data added to the system since the last backup. In addition, without regular backups, the TTC could lose the data recorded in the badge access system's access logs.

As a result of the failure to meet agency and NIST requirements regarding backups of automated information systems, the TTC may not have reliable information system backup information on hand if there is a need for system or file recovery.

RECOMMENDATIONS

The Office of the Inspector General recommends that the Executive Director for Operations:

5. Develop and implement procedures for storing information system backup information offsite in a location, cabinet, or safe that is waterproof and fireproof for at least 14 days or as recommended by the agency.
6. Fully document and implement backup procedures for the badge access system.

3.3 Configuration Management

In order to evaluate the TTC's compliance with the agency's configuration management requirements, the evaluation team asked TTC staff questions about the implementation of the agency's new laptop security policy. The evaluation team also conducted a network vulnerability assessment scan. As the TTC is just beginning to implement the requirements outlined in the new laptop security policy, the evaluation team was unable to form an opinion on its progress. However, the network vulnerability assessment scan identified deviations from the agency's configuration requirements.

Vulnerability Scan Identified Deviations from the Agency's Configuration Requirements

FISMA and NIST SP 800-53 require agencies to develop policies and procedures that ensure compliance with minimally acceptable system configuration requirements as determined by the agency. The NRC's minimally acceptable system configuration requirements are based on various industry standards. However, a network vulnerability assessment scan identified several vulnerabilities that indicate some TTC systems are not configured in accordance with the agency's established configuration requirements.

3.3.1 Configuration Requirements

FISMA requires agencies to develop policies and procedures that ensure compliance with minimally acceptable system configuration requirements as determined by the agency. NIST SP 800-53 requires organizations to (i) establish mandatory configuration settings for information technology products employed within the information system, (ii) configure the security settings of information technology products to the most restrictive mode consistent with operational requirements, (iii) document the configuration settings, and (iv) enforce the configuration settings in all components of the information system.

The agency's minimally acceptable system configuration requirements for the different devices, operating systems, network devices, and applications in use at the agency can be found on the agency's intranet.[4] Hardening standards in use at the agency include the Center for Internet Security and the Defense Information Systems Agency (DISA) Gold Disk[5] benchmarks, National Security Agency security configuration guides, and custom hardening specifications developed by the agency. The agency requires the use of the most recent version of the specified hardening specifications.

3.3.2 Agency Has Not Met Requirements

To determine the extent to which the agency is implementing minimally acceptable system configuration requirements for the different devices, operating systems, network devices, and applications, Carson Associates conducted a network vulnerability assessment scan. The scan was conducted on the TTC's LAN. The scan did not include the network that supports the simulators. The scan identified several vulnerabilities that indicate some TTC systems are not configured in accordance with the agency's established configuration requirements. The following are some examples of the vulnerabilities identified by the network vulnerability scan.

- Dormant accounts – the scan identified 48 accounts on one server that have never logged in. This could indicate dormant accounts. Any account dormant over 35 days is contrary to the agency's hardening standards.
- Minimum password age – the scan identified a server with a minimum password age policy set to 0 days.
- Accounts with passwords that do not expire – the scan identified 15 accounts on one server with passwords that do not expire.
- Guessed password – the scan was able to guess the password to one account (it was the same as the account name).
- SSL[6] certificate issues – the scan identified multiple servers and devices with SSL certificate issues. The scan found SSL certificates that are self-signed where the subject and target of the certificate do not match. The scan also found SSL certificates that accept weak ciphers and accepts the SSLv2 protocol.

These are only some examples of the vulnerabilities identified by the network vulnerability scan. The TTC has been provided with full details on all of the vulnerabilities identified by the scan. For some vulnerability checks, the presence of certain security measures on a target host could cause the scanning software to return a false positive. For other vulnerabilities, it is impossible

[4] http://www.internal.nrc.gov/CSO/standards.html.
[5] The DISA Gold Disk is a tool that allows a system administrator to scan a system for vulnerabilities, make appropriate security configuration changes, and apply security patches. The Gold Disk uses an automated process that configures a system in accordance with DISA Security Technical Implementation Guidelines.
[6] The secure socket layer (SSL) and its successor, transport layer security (TLS), are cryptographic protocols that provide security and data integrity for communications over networks such as the Internet. These protocols allow client/server applications to communicate across a network in a way designed to prevent eavesdropping, tampering, and message forgery.

to determine with certainty whether the vulnerability, in fact, exists merely by probing it remotely. The agency will need to evaluate the scan results to determine which vulnerabilities are false positives.

RECOMMENDATIONS

The Office of the Inspector General recommends that the Executive Director for Operations:

7. Evaluate the vulnerabilities identified by the network vulnerability assessment and develop a plan and schedule to identify any false positives and to resolve the remaining vulnerabilities.
8. Perform a network vulnerability scan following remediation to verify all vulnerabilities have been resolved.

4 Observations

During the course of fieldwork, OIG auditors observed the following issues pertaining to the new physical access control systems recently installed at the TTC. OIG is not making formal recommendations to correct these issues; however, these concerns warrant management attention.

4.1 Password Requirements Are Not Being Met

MD and Handbook 12.5 Appendix A, "NRC Systems Development and Maintenance Security Controls," defines the agency's requirements for identification and authentication controls, including passwords. While evaluating the new badge access system, the evaluation team observed the following deviations from the password requirements set by the agency:

- Users cannot set their own passwords.
- The administrator's password is only four characters in length.
- The administrator's password is not required to be changed periodically.

As the installation of the TTC's badge access system is incomplete, it is possible that these deviations are a result of the delay in completing the installation. However, the agency should correct these deviations when installation of the TTC's badge access system is completed. The agency should also ensure that these deviations are not repeated when the new badge access system is installed in the four regional offices and at headquarters.

4.2 Inadequate Key Management for Physical Access Control Systems' Keys

There are several locked boxes on each floor of the TTC that house components of the physical access control systems that were recently installed. In addition, there are locked boxes in the TTC's main computer room that also house components of the physical access control systems. The vendor left the TTC with keys for the boxes. However, none of the keys were labeled as to which boxes they open, and the TTC is unsure if they received keys for every locked box. When the agency completes the installation of the TTC's badge access system, the agency should ensure the TTC has all the keys to all the locked boxes and that all the keys are properly labeled. The agency should also ensure that the keys are properly labeled and distributed when the new badge access system is installed in the four regional offices and at headquarters.

[Page intentionally left blank]

5 Consolidated List of Recommendations

The Office of the Inspector General recommends that the Executive Director for Operations:

1. Provide comprehensive training on the TTC's new physical access control systems as soon as possible. The agency should not wait until the Division of Facilities and Security returns to install the TTC's badge access system server.
2. Provide comprehensive documentation on the TTC's new physical access control systems as soon as possible. The agency should not wait until the Division of Facilities and Security returns to install the TTC's badge access system server.
3. Complete the hardening of the TTC's badge access system server and install it at the TTC.
4. Activate the TTC's intrusion detection system to sound a local audible alarm until the agency can coordinate with the Federal Protective Service to monitor the alarms.
5. Develop and implement procedures for storing information system backup information offsite in a location, cabinet, or safe that is waterproof and fireproof for at least 14 days or as recommended by the agency.
6. Fully document and implement backup procedures for the badge access system.
7. Evaluate the vulnerabilities identified by the network vulnerability assessment and develop a plan and schedule to identify any false positives and to resolve the remaining vulnerabilities.
8. Perform a network vulnerability scan following remediation to verify all vulnerabilities have been resolved.

[Page intentionally left blank]

Appendix. SCOPE AND METHODOLOGY

The scope of this information system security evaluation included:

- The four floors the TTC occupies in the Osborne Office Center located at 5746 Marlin Road, Chattanooga, TN 37411-5677.
- TTC LAN equipment.
- IT equipment supporting TTC automated information systems.

The information system security evaluation did not include controls related to the management of safeguards or classified information. The evaluation also did not include IT equipment and applications supporting the simulators.

Carson Associates performed the information system security evaluation of the TTC. In conducting the information system security evaluation, the following areas were reviewed: security policies and procedures, automated information systems inventory, physical and environmental security controls, continuity of operations and emergency planning, configuration management, and LAN administration. Specifically, the evaluation team conducted site surveys of the four floors the TTC occupies in the Osborne Office Center located at 5746 Marlin Road, Chattanooga, TN 37411-5677, focusing on the areas that house LAN equipment and IT equipment supporting local automated information systems. The team conducted interviews with the TTC Information System Security Officer, the LAN administrator, and other TTC staff members responsible for implementing the agency's information system security program. The evaluation team also conducted user interviews with 10 TTC employees. The team reviewed documentation provided by the TTC, including floor plans; network diagrams; inventories of automated information systems, hardware, and software; local policies and procedures; security plans; contingency plans; backup procedures; and the Occupancy Emergency Plan. The information system security evaluation also included a network vulnerability assessment scan of the TTC's LAN. The scan did not include the network that supports the simulators.

All analyses were performed in accordance with guidance from the following:

- National Institute of Standards and Technology standards and guidelines.
- NRC MD and Handbook 12.5, *NRC Automated Information Security Program.*
- NRC Office of the Inspector General audit guidance.

This work was conducted during a site visit to the TTC between May 11, 2009, and May 14, 2009. The work was conducted by Jane M. Laroussi, CISSP, and Virgil Isola, CISSP, from Richard S. Carson and Associates, Inc.

[Page intentionally left blank]